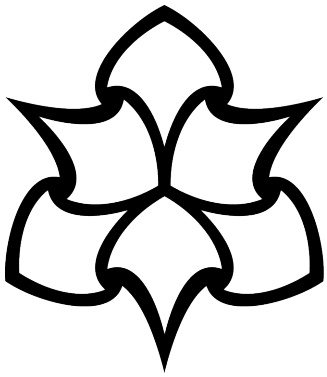

A state of the art survey - Impact of cyber attacks on SME's

Jibran Saleem
Cyraatek
Unit 17, Waters Edge Business park
Modwen Road, Salford, M5 3EZ
js1010@cyraatek.com

Bamidele Adebisi
School of Engineering, Manchester Metropolitan University
Manchester
B.Adebisi@mmu.ac.uk

Ruth Ande
Cyraatek
Unit 17, Waters Edge Business park
Modwen Road, Salford, M5 3EZ
ruth@raatek.co.uk

Mohammad Hammoudeh
School of Computing, Mathematics, & Digital Technology, Manchester Metropolitan University
Manchester
M.Hammoudeh@mmu.ac.uk

ABSTRACT

Corporations and end users are finding it hard to keep their devices safe from the ever evolving and complicated threat of cyber attacks. Currently, with the widespread adoption of the Internet of Things (IoT), cyber threat is becoming an even greater challenge for both technology providers and consumers. This paper presents a review of the recent and significant cyber security issues affecting many areas of digital technology. From IoT devices and smart automobiles to commonly used computers and typical corporate servers, we focus our analysis on current attack trends and the effects of intrusion on Small and Medium sized Enterprises(SMEs). This paper helps to build awareness among non-technical experts, practitioners and researchers about attack and defense strategies in the current digital market. We have created a guide with input from our in-house security researchers and information gathered from the literature to help the reader understand the challenges faced by the IT industry in the future.

CCS CONCEPTS

•**Security and privacy** → **security services;** *Intrusion/anomaly detection and malware mitigation;* •**Computer systems organization** → Dependable and fault-tolerant systems and networks; •**Networks** → Network reliability;

KEYWORDS

Cyber Threats, Computer Security, IoT, Privacy, Security Audit, Penetration Testing, Security Analysis

ACM Reference format:
Jibran Saleem, Bamidele Adebisi, Ruth Ande, and Mohammad Hammoudeh. 2017. A state of the art survey - Impact of cyber attacks on SME's. In *Proceedings of ICFNDS '17, Cambridge, United Kingdom, July 19-20, 2017,* 7 pages.
DOI: 10.1145/3102304.3109812

ICFNDS '17, Cambridge, United Kingdom

DOI: 10.1145/3102304.3109812

1 INTRODUCTION

Computers have revolutionized our lives since the day they came into existence. From putting a man in space, to performing automated complex medical surgeries, helping people shop on-line from the comfort of their homes as well as enabling us to reach out and connect to our loved ones through social media, digital technology is assisting us in every aspect of our lives. Therefore, it is undebatable that computers are now an integral part of human life. However, this necessity of life has also attracted great interest from malicious attackers, informally referred to as hackers, who perform many attacks in this illegal trade to bring harm to the ordinary users, or financial gain to themselves. Many enterprises fall victim to these attacks and face substantial financial losses, data breaches and subsequent lawsuits, resulting in further financial implications [5]. For example, a report released by McAfee in 2014 titled "Net Losses: Estimating the Global cost of Cybercrime" [16] predicted that the annual estimated losses to Global economy due to cybercrimes could be as high as $575 billion in 2015. Further analysis conducted by a firm "Cyber Security Ventures" in 2016 concluded [21] that the total global cost of cyber crimes would reach around $3 trillion by 2015 and could be as high as $6 trillion by 2021.

Digital attacks against Small and Medium sized Enterprises (SMEs) are so frequent that they are now considered a common occurrence worldwide:

(1) Due to the fact that small enterprises under appreciate the threat of cyber security,
(2) SMEs have limited funds to implement security efficiently,
(3) There is an immense shortage of skilled security workers, which is having an effect on business who want to bolster their network against attacks,
(4) Lastly, the soaring cost of security auditing solutions and security awareness training for employees is another reason why some SMEs have not deployed effective digital defences against attackers [13].

The ultimate purpose of this paper is to enable SME's to understand the impact of cyber threats and the difficulty that they may potentially face in the future if precautionary measures are not put in place to secure their IT infrastructure. Additionally, this paper also lists several assessments, with regards to the direction in which

the cyber threat will move, due to the sweeping adoption of IoT devices.

The rest of the paper is organised as follows: Section 2 discusses the ever-evolving threats of Cyber security whereas Section 3 evaluates the challenges technology users are now faced with due to the implementation of lax security protocols in IoT devices. Section 4 details mitigation methods SMEs can adopt to protect themselves from the cyber attacks. Section 5 sheds further light on current cyber attack trends. Section 6 and 7 lists benefits of regular penetration testing exercises and future threat predictions relating to Cyber attacks. Finally concluding remarks are presented in Section 8 of the paper.

2 UNDERSTANDING THE COST OF CYBER ATTACKS ON ENTERPRISES

Recent research undertaken by the UK Government [15] revealed that nearly two thirds of large businesses suffered an attack or an IT related breach on their equipment in 2015. The same article refers to the UK Government's strategy to combat cyber attacks by dedicating $2.4 billion in investment, to bolster IT infrastructure as well as funding a new 'National Cyber Security Centre', which was inaugurated by the Queen in February 2017.

However, despite all the measures being taken at a higher level, the threat of digital attacks against businesses is likely to intensify[2]. The threat of cyber attacks is at an all time high, and our analysis of trends indicates that it will continue to rise.

Cyber attacks against technology users of all types and businesses of all size are on constant increase. The attacks are getting more sophisticated in nature [14]. Consequently, it is becoming harder for businesses to stay on top of this threat as some attackers have devised complex techniques to enable them to stay unnoticed and unidentified. For example, WannaCry ransomware attack, which occurred in May 2017, made use of sophisticated exploits, first identified by U.S. National Security Agency (NSA). By exploiting unpatched vulnerabilities in older, unsupported operating systems, this variant of ransomware quickly spread across many networks, encrypting all the data in the process and making all affected computers unusable.

Allianz Insurance, one of the top players in the UK insurance industry, annually issues a report on the threats faced by modern world. Their 2016 report [1] claims that the cyber related incidents have increased by over 17% compared to 2015, making it one of the largest threats businesses are facing today.

The exponential increase in the use of cloud and mobile technologies as well as IoT is making a considerable impact on the digital device users. The growth in IoT is not only providing enterprises with an opportunity to design more energy efficient devices, the increase in widespread adoption of IoT has also increased the competition in the market, which in turn has had a positive impact and made products more affordable for the consumers. However, continued evolution of these services has also brought many security challenges for the users of these technologies. Fundamentally, a lack of awareness about rapidly evolving security issues is the reason most users and companies are failing to protect themselves from cyber attacks.

Rapid expansion of IoT devices coupled with inadequate security mechanisms employed by these devices, will lead to substantially greater cyber security risks in the near future. The consequences of exploitation on such technologies will have drastic effects, not just on businesses but all technology users, from individuals to governments [6]. The lack of awareness with regards to IoT security, among its users, is a major concern for cyber security experts.

3 EMERGING THREATS AND CHALLENGES — INTERNET OF THINGS

IoT is the Internetworking of physical devices, comprising of everyday objects (i.e., fridge, toasters, lights, medical devices, identification tags), with sensors and network connectivity that enable these objects to collect and exchange data. IoT is a pervasive technology, which spans across many sectors. Today, it is not uncommon to see lights that can turn on automatically when they detect your presence, or fans that can switch on if the temperature exceeds a set amount. Similarly, we now have products in the market like smart kettles, that can be activated remotely with a touch of a button on a mobile phone, or location aware thermostats, that can turn the heating on when they detect you are leaving office for home and always-on voice activated virtual assistants, with the ability to carry out precise data analysis to support us in our daily tasks. Recent introduction of Amazon Dash button for example, brings convenience and ease in the lives of many of their customers. Rather than looking for a smartphone, tablet or a computer to order items, Amazon customers can simply press the wirelessly connected standalone button, which then sends a 'purchase'command to Amazon, so delivery of the pre-specified goods, for example a regularly consumed product like toilet paper, can be arranged.

We are now completely surrounded by IoT devices. In Smart Cities, for example, IoT devices are used to manage smart parking, traffic congestions, and lighting and to study changing habits of urban population. Smart sensors are being used to measure temperature inside industrial and medical storage facilities containing sensitive merchandise. IoT devices with auto diagnosis capabilities are being used in vehicles to send real time alarms to emergency services, in the case of an incident.

The reality is that the IoT industry is expanding rapidly. According to Gartner Inc. [12] there will be 21 billion connected IoT devices by the end of 2020. Forbes reports that the number [7] the IoT devices will reach 75.4 billion by 2025.

Analysis of the reports relating to this industry shows that the exponential growth in the IoT device uptake has taken academics, scientists and technology sector in general, by surprise. The large-scale adoption of IoT is having a similar effect on the IT industry and consumers as the Iphone had, when it was first launched in summer 2007. However, in the case of IoT, no one anticipated that this industry could become so huge relatively overnight. Although, it can be argued that devices connected to wireless Internet has now been in existence for well over two decades, [3] it is only in the last three to four years that we have observed a huge rise in their uptake, within the consumer market, transforming everyday objects into smart devices. However, sudden growth and adoption of IoT in the past few years has also given rise to new attack vectors.

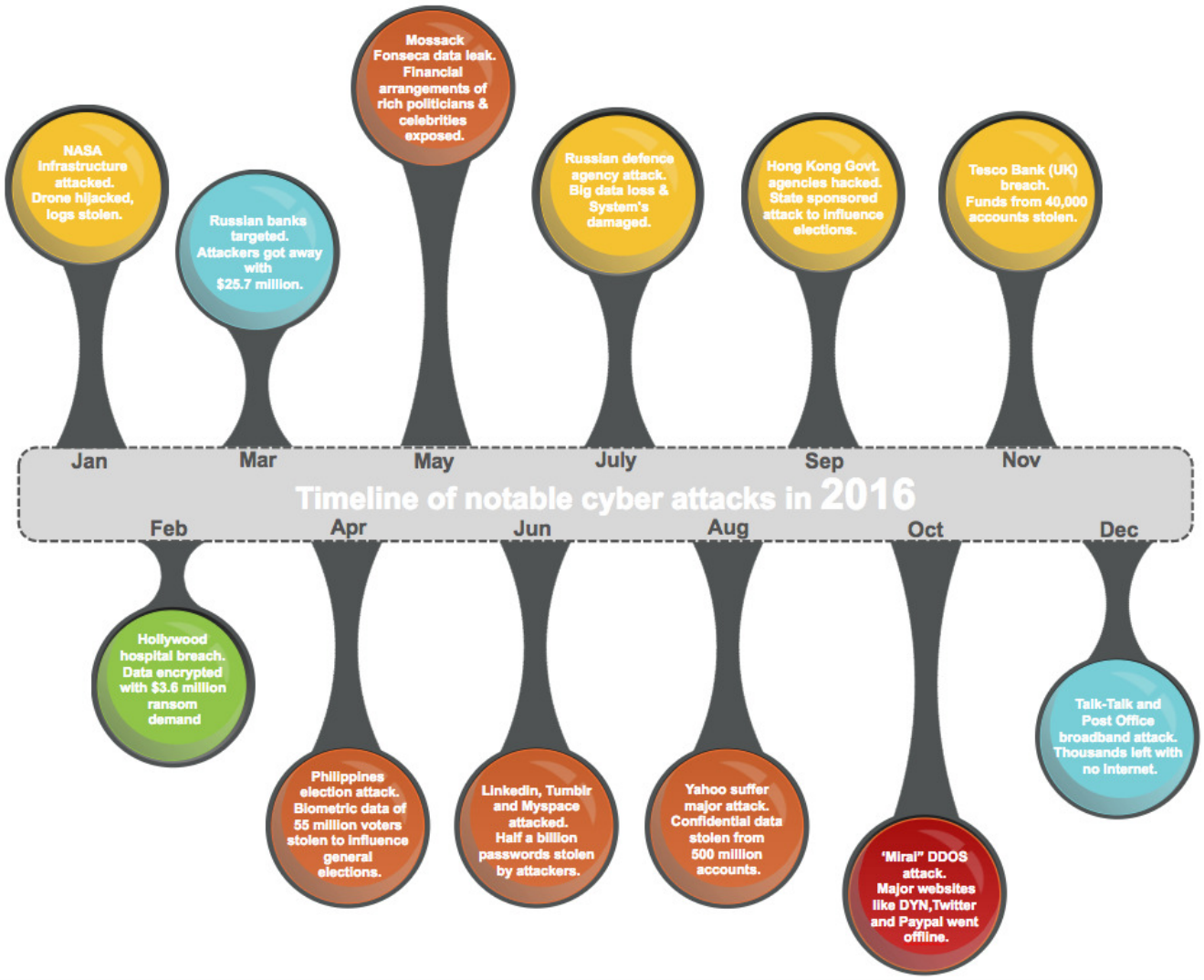

Figure 1: Time-line of notable Cyber Attacks in 2016.

The problem with IoT sector is not its rapid growth, but the lack of security within devices, and in the way they connect to the Internet. After thorough analysis of varying types of IoT devices, there is a mutual consensus between academics, researcher and ethical hackers that objects bearing IoT hallmarks have generally much weaker security compared to computing devices we traditionally use [20].

The most recent result of such security lapse is the outage of some of the top Internet websites, occurring in October 2016 [19]. A timeline of memorable cyber attacks that occurred in 2016 can be viewed in 'Figure 1', including the infamous'Mirai 'attack. Attacks with most severe impact are represented with darker colours and longer branches.

Experts describe the Internet outage caused by Mirai to be one of the largest and most organized of its kind in the Internet history. To facilitate the offensive, attackers hacked a large collection of IoT devices using a malware, known as 'Mirai ', which utilised computational brute force and dictionary attack methods to break into poorly secured IoT devices. Once in control, the malware further infected the devices with malicious code so they could be turned into bots, which could then perform a variety of automated tasks on behalf of their masters. A bot is a short name for 'robot'. The computer bots have the ability to perform automated tasks and can operate over the Internet as well as offline.

A large collection of bots is all the hackers needed to launch their attack. The botnets were used to direct massive amounts of bogus Internet traffic (approximately 990Gbps) towards the infrastructure of Dyn, an Internet performance management company and a cloud service provider, allowing the hackers to send Dyn's servers off-line for considerable amount of time. Consequently, companies who relied on Dyn for their services, also went off-line for the duration of the attack. Some of the well-known companies that became

victims of this attack included Reddit, Paypal, Twitter and Spotify, among many others.

The above example affected companies and their service provision, but the danger of IoT hacking can be life threatening in some cases. For instance, imagine hackers taking control of the medical devices embedded in humans, to assist them with their bio-functions. Once a session is established between a hacker and medical IoT device, hackers could relatively easily disturb digital mechanics of the device and intentionally or unintentionally cause damage or even death to the wearer. For example, the Food and Drug Administration (USA) [10] released a statement in February 2017, in which they warned that some pacemakers are vulnerable to hacking. The advisory stated that under certain conditions, attackers could take complete control of the pacemaker, send modified commands to the device, in order to achieve complete battery depletion and even administer inappropriate pacing or shocks to the wearer.

There have also been reports in the media relating to successful unauthorised takeover, by security researchers and malicious attackers, of autonomous and semi-autonomous auto-mobiles and even drone aeroplanes, in the recent months. Autonomous cars rely heavily on wireless networks and satellites to perform their functions. By using unsecured and weak methods of communications, manufacturers of autonomous cars could be inadvertently putting the users in danger.

Wired, a reputable news source among technology enthusiasts, reported about a hack conducted by two security researchers on Chrysler's Jeep Cherokee in 2016. During the experiment the researchers determined that, by sending carefully crafted messages to the vehicle, they could send remote commands to the vehicle to perform dangerous manoeuvres including rapid acceleration, harsh braking and even the controlling vehiclefis steering wheel at any speed.

By utilising zero day exploits, which are security flaws that were not previously known, hackers are now successfully chartering this previously invulnerable territory of drone and smart car attacks. We anticipate these type of attacks will become an even bigger problem for manufacturers, users and governments, compared to attacks on small immobile devices.

In march 2016, the Federal Bureau of Investigation released a public service announcement (I-031716-PSA) [9] in which it warned that modern motor vehicles are increasingly susceptible to remote exploits and urged the consumers to be cautious and recommended measures to minimise the possibility of an attack.

Increasing interest from hackers in IoT devices suggests that the October 2016 Mirai attack [19] was just the beginning. A hacked IoT system can also potentially be used as a gateway to any other devices that are connected to the same network, for example smart mobile phones, or enterprise infrastructures. Once attackers are inside an IoT system, attackers have the ability to transmit malicious code through the IoT communication system to the connected devices or systems. We anticipate IoT hacking will become a more mainstream route of attack among hackers. To defend against this, all IoT device developers and manufacturers are encouraged to give these vulnerabilities their attention during device and network development phase.

Moving forward, ultimately consumers of IoT products also have a responsibility to play their part in securing their devices. When it comes to smart devices, it is clear that some manufacturers are slow in issuing critical software updates. These updates are generally an efficient way to patch known bugs and vulnerabilities. However, if a device is already exploited by an attacker, it is probable that the attacker will set the device to refuse any manufacturer updates to allow the hacker to continue with maximum control over the device. In this scenario, it is the responsibility of the device's user to check that their devices are up to date with manufacturer updates and that they are not being manipulated, for example not being used as a botnet or as a surveillance device. Devices including virtual assistants, for example Amazon's Echo and Google Home, are increasingly becoming part of a normal household. These assistants contain an always-on microphone, and they have the potential to act as an excellent spying device for an attacker. In addition, customer data and search history are stored on these devices. If not protected, this data can easily be obtained by attackers, providing them with useful information about the habits and routines of a household.

In March 2017, Wikileaks [22] claimed in leaked intelligence documents that the CIA is running a secret computer hacking programme, providing its agents with tools to hack and listen into everyday devices such as TVs, phones and tablets. The report also mentions that the CIA has acquired the capability to target cars, which are operated by onboard computers with Internet connectivity. Wikileaks further claimed that once in control of the vehicles, the CIA could stage a crash, resulting in an assassination but making the crash appear to be an accident.

Following this revelation, Wikileaks began dumping these CIA hacking tools on the Internet, in the hope that manufacturers would study these exploits and take measures to ensure that these vulnerabilities are patched. Instead, these hacking tools have ended up in public domain and are being accessed by malicious hackers, who have now used them to develop stronger attack capabilities aimed at everyday smart devices. Most recently, hackers made use to these tools to launch a ransomware attack on major institutions. The malware named "WannaCry" made headlines across the globe after infecting and encrypting hundreds of thousands of computers overnight in May 2017.

4 MITIGATION METHODS

In order to protect themselves, as a minimum, enterprises need to adhere to security standards [4]. The four steps below are given to enable this adherence, helping you to check that your smart devices are safe and secure:

(1) Make sure that Internet connected devices, connected networks and operating software are running the most up to date patch that is issued by the manufacturer.
(2) Ensure that all communications and data transfer over the network is encrypted. This allows the user to create a barrier between themselves and an attacker.
(3) It is also strongly recommended that a strong password be used wherever possible. Readily available hacking tools can easily crack weak passwords. A strong password is usually defined as having a minimum length of at least

twelve characters, comprising of unique mixture of letters, numbers and symbols. This will significantly reduce the risk of devices being hacked by an attacker.

(4) Use multi-factor authentication for critical devices and infrastructure to stop unauthorised access. Dual layer authentication is also an excellent mitigation mechanism to repel brute force attacks.

Periodic penetration testing exercises from an accredited security auditing company is also recommended, as these tests can substantially enhance chances of discovery of any potential anomalies or holes in the security of smart devices or the systems they are connected to. By simulating a real-world attack scenario, a penetration test can determine the vulnerabilities that exist in your systems, enabling you to take preventive action and understand and improve your ability to deal with the attack, if it occurs.

5 ANALYSIS ROUNDUP

Dell is one of the most recognisable names in the IT industry, serving corporations and end users of all types. The annual cyber security threat report published by Dell in 2016 [8] shows a worrying but unsurprising surge in the cyber crimes being committed across the globe. Their report demonstrates the severity and magnitude of the ever-increasing attacks on big names, such as Amazon, Bank of Scotland, Ashley Madison, Harvard University and many more. Overall, the report by Dell presented an alarming rate with which viruses, trojans and increasingly sophisticated exploit kits are being used to target computing and IoT devices. However, critical servers currently remain the primary target of the attackers in the category of intrusion attacks.

Another company, FireEye, which focuses exclusively on the cyber security, published their report in early 2017 [11] on the emerging trends in attack methodology employed by malicious attackers and digital defence strategies. Commenting on the rise of sophisticated attack methods, the editor of the report states:

"Financial attackers have improved their tactics, techniques and procedures (TTPs) to the point where they have become difficult to detect and challenging to investigate and re-mediate." [11]

Research conducted by FireEye highlights how scammers are changing their tactics to bypass complex authentication protocols. For instance, attackers are increasingly developing malicious applications that can overcome two-factor authentication requirements by embedding malicious applications with Open Authentication (OAuth) tokens. OAuth is an open-source standard and is widely used by developers to obtain authority to share information without the need for a password. As soon as a victim mistakenly authorises the malicious application's request for access, the attacker acquires the ability to gain entry to all data held on victim's account, for example their Google account, and can retain permission to access the account, even when the password is updated or changed.

Infosecurity, Europe's largest Security event organiser, recently stated in their magazine that following comprehensive research, evidently hackers spend on average 200+ days inside an IT system before being discovered. [18]

By any measure, two hundred days is a considerable amount of time for anyone to monitor servers, to extract and analyse data. However, the same article also states that the discovery of a breach after intrusion occurred used to be around 243 days in 2012. Hence, we are making progress when it comes to attacks being detected and remedied. This improvement can be associated with a small increase in the level of awareness of security threats. In addition some enterprises, particularly larger enterprises are now using security auditing services, which are being offered and promoted more, compared to the past.

The growth of IoT and mobile devices, with the capability of exchanging data over the Internet, has created the biggest digital attack vector known to the technology industry in recent history. While it is probable that with education and persistent reminders, IoT developers will start taking security more seriously, evidence suggests that it has not happened yet. Which is why an estimated 8 billion currently connected IoT devices [12], a figure that is set to rise to 75 billion by 2025 [7], pose a significant cyber risk to the global digital infrastructure. Current attack trends should lead companies to re-think their defence strategies in the face of repeated cyber threats. As a minimum, SMEs should adhere to security protocols and offer security training to their staff. In addition, SMEs should consider committing to regular security auditing and penetration testing exercises, as well as improving staff awareness on security issues, to prevent them from becoming a victim of social engineering attacks.

Governments and regulatory bodies can also play a major role by introducing laws and policies to ensure IoT products are not released to the masses, unless they meet stringent security standards. By taking these measures, governments will not only play their part in making Internet a safe space for everyone, but will also see a reduction in their own cyber investigation's bill after the aftermath of a cyber attack. The next section of this white paper has shed some light on the benefits of regular penetration testing.

6 VALUE OF PENETRATION TESTING

In today's convoluted security landscape, it can be hard for businesses to keep track of all the emerging threats. As more and more zero day exploits are exposed by the researchers, it is more important than ever to have an understanding of what problems a business might suffer if they face an attack on their infrastructure.

During an attack, companies may suffer loss of their services. In the aftermath of the attack, as well as suffering loss of reputation, companies can also receive fines from regulatory authorities for failing to take sufficient steps to protect their systems, losing customer data, as well as the possibility of lawsuits from their customers. So, to protect oneself from the possibility of an attack, penetration testing is an exercise, which is undertaken by security professionals on behalf of a company to determine and assess vulnerabilities in a system.

Penetration testing is essentially a practise of testing computer systems against known technical weaknesses, to determine the type of vulnerabilities residing in the software, hardware and web applications. The main purpose is to find vulnerabilities and make it more difficult for malicious attackers to gain unauthorised access to IT infrastructures and private data. After completion of the testing, the penetration test will present a detailed report with a list of all vulnerabilities identified during the testing and a set of

recommendations. This report enables the host company to fix or patch any technical or procedural weakness in their infrastructure.

6.1 A CLOSER LOOK AT THE ADVANTAGES OF PERIODIC PENETRATION TESTING

It is reported by Navigant [17], who operates as a specialised expert service firm, that the average cost of security breach in 2013 was $4,976,900. Navigant also reported that security testing performed by 'Cenzic Security'in the same year, led to discovery of technical flaws in 96% of the cases. An average loss of $4,976,900 is a substantial amount, in contrast, security testing would only cost a fraction of this amount. These incredible statistics demonstrate a strong case for why corporations must integrate regular penetration testing into their security procedures.

It is recommended that a security evaluation is requested periodically, especially during the creation of a new infrastructure or during every significant alteration to an organisation's IT infrastructure. If the evaluation cannot be carried out during an alteration phase, it should be carried out after its completion to highlight any new vulnerabilities. A detailed penetration test provides the following benefits to the client:

- Testing of defence capability: A penetration test not only reveals the flaws that can be exploited by the attacks, but the assessment can also help the organisation assess their readiness to deal with a breach, should an attack occur.
- Achieving certifications and compliance with geographical, industry or legal regulations: There is often a legal requirement for corporations and businesses to perform penetrations tests against their information systems before they can apply for certifications, such as ISO27001. Therefore, security testing should be carried out to facilitate this compliance. The Security testing can include testing for this specified certifications, if required.
- Protecting data, clients and reputation: When businesses consider the cost of penetration testing, this should be compared against the cost of the loss of service or business continuity, potential loss of data, damage to reputation and subsequent lawsuits and fines that would result if a breach occurs.
- Market competition: To be competitive in the market, SMEs often have to demonstrate to their customers that they have taken sufficient security precautions to ensure protection of data and have established disaster recovery plans. A certificate of completion in security auditing and penetration test can help assure customers that a responsible company is looking after their affairs.
- Risk Assessment: It is important for SMEs to use risk based thinking with a good understanding of information security and why it is crucial for business operations. Penetration testing can help businesses understand the weaknesses in their technical infrastructure. The report, which is provided comprises of an extensive list of recommendations that enterprises can implement to harden their system against malicious attackers. This list of recommendations will be graded to differentiate the effect that each recommendation will have on the system.

In short, corporations need to go above and beyond normal business practices to stay on top of security threats, which are continually evolving. The security challenges in today's digital world are dynamic, daunting and convoluted. Therefore, robust cyber security, continual testing of infrastructure and regular training regarding the security outlook of employees should be the top priority of all businesses that have an IT infrastructure, not just those who are security conscious. A holistic and comprehensive strategy that deals with risk management, cyber security and continuous penetrations testing, will help the businesses in protecting themselves from the dangers of cyber attacks.

7 CYRAATEK'S CYBER THREAT PREDICTIONS FOR YEAR 2020

This section offers short to long-term insight for companies looking to stay ahead in the race against attackers. The content below predict key development and forecast trends that are likely to occur over the next few years.

(1) Ransomware: The availability of various beginner-friendly ransomware deployment kits has enabled even the low-tech criminals to enter sphere of cyber crime. This is likely to cause further increase in ransomware attacks on technology users of all types. Recent 'WannaCry'ransomeware attack is the primary example of such cases where readily available complex exploits are being used by criminals to launch large-scale attacks with relative ease.
(2) Increase in data breaches: With recent attacks on LinkedIn, Target, Wonga, NSA, Cloudflare, CloudPets and many more, attackers are actively targeting institutions for information. We anticipate that in the coming years, this trend is likely to continue with many more organised cyber assaults on consumer data companies.
(3) Phishing attack: SaaS cloud model is susceptible to phishing and server cracking attacks. Over the years, we have seen advances in complexity of phishing attacks. Criminals now have the ability to forge SSL certificates, which renders built-in browser protection against phishing useless. Because of the ease with which certificates can now be forged, we predict substantially more attacks, as more businesses move their data to the cloud.
(4) Increase in state-sponsored attacks: In the light of Stuxnet, The Shadow Broker's leaks and the North Korea hack's for example, we will continue to witness increase in reported state-sponsored attacks as Government's desire to know more about what their enemies and allies are doing.
(5) Smart grid attacks and IoT: In the recent years, there been a significant rise in the adoption of smart grid and IoT devices. Many cities are now competing with each other to implement smart features in their infrastructure. However, this technology suffers from serious vulnerabilities. As the uptake of this technology increases, attackers will have even greater availability of vulnerable of appliances and devices, which they will potentially hack for malicious purposes.

8 CONCLUSIONS

To protect oneself from ever increasing threats of cyber attacks, enterprises and users of technology need to be ready with concrete defence strategies since the cyber threat landscape is continually evolving in complexity. By efficiently utilising technical and human resources to protect the network and connected devices, companies will not only protect themselves from harm and potential financial loss, but also play their part in making cyberspace more secure and safe for online users. In conclusion, the more enterprises learn about threat prevention, detection and response, the faster they will become at preventing and mitigating cyber attacks.

ACKNOWLEDGMENTS

This work was funded by Innovate UK as part of the "KTP - Knowledge Transfer Partnership" (Innovate UK project number 1022602).

REFERENCES

[1] Allianz. 2016. Two thirds of large UK businesses hit by cyber breach or attack in past year. =http://www.agcs.allianz.com/global-offices/united-kingdom/news-press-uk/allianz-risk-barometer-2016-press-uk/. (2016). [Online; accessed 8-June-2017].

[2] Arwa Alrawais, Abdulrahman Alhothaily, Chunqiang Hu, and Xiuzhen Cheng. 2017. Fog Computing for the Internet of Things: Security and Privacy Issues. *IEEE Internet Computing* 21, 2 (2017), 34–42.

[3] Kevin Ashton. 2009. That fiinternet of thingsfi thing. *RFiD Journal* 22, 7 (2009), 97–114.

[4] Andrew Carlin, Mohammad Hammoudeh, and Omar Aldabbas. 2015. Defence for Distributed Denial of Service Attacks in Cloud Computing. *Procedia Computer Science* 73 (2015), 490–497.

[5] Andrew Carlin, Mohammad Hammoudeh, and Omar Aldabbas. 2015. Intrusion detection and countermeasure of virtual cloud systems-state of the art and current challenges. *International Journal of Advanced Computer Science and Applications* 6, 6 (2015).

[6] Abdullahi Chowdhury. 2017. Cyber attacks in mechatronics systems based on Internet of Things. In *Mechatronics (ICM), 2017 IEEE International Conference on*. IEEE, 476–481. [Online; accessed 8-June-2017].

[7] Louis Columbus. 2015. Roundup Of Internet of Things Forecasts And Market Estimates, 2015. =https://goo.gl/I90ewy. (2015). [Online; accessed 8-June-2017].

[8] Dell. 2016. Dell Security Annual Threat Report 2016. =http://www.netthreat.co.uk/assets/assets/dell-security-annual-threat-report-2016-white-paper-197571.pdf,. (2016). [Online; accessed 8-June-2017].

[9] FBI. 2016. Public Service Announcement. =https://www.ic3.gov/media/2016/160317.aspx,. (2016). [Online; accessed 8-June-2017].

[10] FDA. 2016. Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin. =https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm.. (2016). [Online; accessed 8-June-2017].

[11] FireEye. 2017. M-Trends 2017 Cyber Security Trends. =https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html,. (2017). [Online; accessed 8-June-2017].

[12] Gartner. 2016. Gartner Says Organizations Must Update Their Network Access Policy to Address Attack of IoT Devices. =http://www.gartner.com/newsroom/id/3436717. (2016). [Online; accessed 8-June-2017].

[13] Ibrahim Ghafir, Vaclav Prenosil, Ahmad Alhejailan, and Mohammad Hammoudeh. 2016. Social engineering attack strategies and defence approaches. In *Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on*. IEEE, 145–149.

[14] Ibrahim Ghafir, Vaclav Prenosil, and Mohammad Hammoudeh. 2016. Botnet Command and Control Traffic Detection Challenges: A Correlation-based Solution. (2016).

[15] Gov.co.uk. 2016. Two thirds of large UK businesses hit by cyber breach or attack in past year. =https://www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year. (2016). [Online; accessed 8-June-2017].

[16] McAfee. 2014. Estimating the global cost of cybercrime. https://www.mcafee.com/de/resources/reports/rp-economic-impact-cybercrime2.pdf. (2014). [Online; accessed 19-July-2017].

[17] Navigant. 2014. Cyber Security Trends for 2014. =http://www.navigant.com/insights/hot-topics/technology-solutions-experts-corner/cyber-security- trends-2014-part-1/,. (2014). [Online; accessed 8-June-2017].

[18] Infosecurity Magazine Phil Muncaster UK / EMEA News Reporter. 2015. Hackers Spend Over 200 Days Inside Systems Before Discovery. =https://www.infosecurity-magazine.com/news/hackers-spend-over-200-days-inside/,. (2015). [Online; accessed 8-June-2017].

[19] Naked Security. 2016. Mirai, Mirai, on the wall fi?! through the looking glass of the attack on Dyn. =https://nakedsecurity.sophos.com/2016/10/24/mirai-mirai-on-the-wall-through-the-looking-glass-of-the-attack-on- dyn/. (2016). [Online; accessed 8-June-2017].

[20] Financial Times. 2016. Connected devices create millions of cyber security weak spots. =https://www.ft.com/content/a63b2de8-992c-11e6-8f9b-70e3cabccfae. (2016). [Online; accessed 8-June-2017].

[21] Cybersecurity Ventures. 2016. Hackerpocalypse Cybercrime Report. =http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/. (2016). [Online; accessed 8-June-2017].

[22] Wikipedia. 2017. Vault 7: CIA Hacking Tools Revealed. =https://wikileaks.org/ciav7p1/index.html,. (2017). [Online; accessed 8-June-2017].